EXHIBIT 7

SENATE JUDICIARY COMMITTEE
Senator Joseph L. Dunn, Chair
2005-2006 Regular Session

SB 355 S
Senator Murray B
As Amended March 29, 2005
Hearing Date: April 5, 2005 3
Business & Professions Code 5
AMT:cjt 5

SUBJECT

Anti-Phishing Act of 2005

DESCRIPTION

This bill would prohibit "phishing," the act of posing as a legitimate online company in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information.

The prohibitions of the bill would be enforceable through a suit brought by the Attorney General or a district attorney, or by an individual, Internet service provider (ISP), Web site owner, or trademark owner who was adversely affected by a violation of the Act. Remedies would include the greater of actual damages or $500,000 per violation. Treble damages would be permissible for a "pattern or practice" of violations. Attorneys' fees could be awarded to the prevailing party.

BACKGROUND

"Phishing" is a widespread technique for obtaining personal information, and is used to facilitate identity theft and other crimes. Phishers use fraudulent emails or Web sites to trick consumers into providing personal information, such as bank account numbers and social security numbers, to what is believed to be a legitimate company. The author explains:

> Customers often receive a legitimate looking

(more)

> email that appears to be from their bank or [a] retailer with whom they do business. The consumer is often told via e-mail that a review of their account found "unusual activity" and directs them to a phony website where they are compelled to provide personal information such as their name, account number and other relevant data. Criminals have become very good at mimicking legitimate emails and setting identical Web sites.

CHANGES TO EXISTING LAW

1. Existing law does not regulate "phishing" actions, but makes fraud actionable where the following has been established: (1) a misrepresentation; (2) knowledge of falsity; (3) intent to defraud, i.e., to induce reliance; (4) justifiable reliance; and (5) resulting damage. [Robinson Helicopter Co., Inc. v. Dana Corp. (2004) 34 Cal. 4th 979, 990.]

   This bill would make it unlawful for a person to use a Web page, email, or the Internet to misrepresent that he or she is an online business (e.g., to indicate that he or she is or represents an online business without authorization from that business) and solicit or induce another person to provide his or her personal information.

2. Existing law provides that an attorney general or district attorney can seek an injunction and civil penalties of up to $2,500 per instance for any unlawful business act or practice. [Bus & Prof Code 17200, 17204, 17206.] An individual may seek an injunction for an unlawful business act or practice if he or she suffered an injury in fact and lost money or property as a result. [Bus & Prof Code 17204.]

   This bill would permit the Attorney General or a district attorney to bring an action against a person who violates the Anti-Phishing Act. An individual, ISP, Web page owner, or trademark owner who was adversely affected by a

violation would also be permitted to bring an action. But the bill specifies that an individual may only bring an action against a person who has directly violated the Act.

This bill would permit recovery of remedies that include injunctive relief and the greater of actual damages or $500,000 per separate violation. The bill would specify that multiple violations resulting from "any single action or conduct" only constitute one violation.

This bill would permit a court to award damages up to three times the amount of damages otherwise recoverable when it is established that a defendant has a "pattern or practice" of violating the Act.

This bill would permit a prevailing party to seek attorneys' fees and costs.

COMMENT

1.Stated need for the bill

The author states:

> According to the FBI and the Internet Crime Complaint Center, 78% of all criminal "phishers" are located in the United States. Of these, 15% of all phishing scams originate in California, the most in the nation. In 2004 alone, there were over 100,000 reports of this fraud with over 76,000 consumers losing money. In reported cases alone, consumers lost over $193 million in 2003 and 2004.

The California Alliance for Consumer Protection notes it has received numerous complaints in recent weeks from consumers who filled out forms on false "EBAY web pages" with their personal information, thinking that those pages were authentic.

The Computing Technology Industry Association (CompTIA) states:

> Billions of dollars of Californian commerce, jobs and productivity gains are tied to the spread of Internet commerce and communications. Confidence in the integrity of personal information transmitted via the Internet remains an integral part of the medium's development. However, recent independent studies, polls and national news reports reveal that phishing is greatly undermining that confidence - phishing tops the concerns of many inside and outside of the IT industry as potentially hobbling the Internet's exciting growth.

CompTIA notes that SB 355 "puts real 'teeth'" into its prohibitions by making each separate violation punishable by $500,000 in damages, and tripling damages where a pattern of phishing has been established.

Microsoft states it is important to enact legislation to combat the threat of phishing, in addition to using other tools such as technology innovation, targeted enforcement, and user education. Microsoft contends that the "[s]trong laws and adequate enforcement" provided by SB 355 will be critical to addressing the phishing problem.

2.The term "online business" needs definition

Since the prohibitions of this bill are limited in application to those who pose as an "online business," this term needs to be defined. The author has committed to work with industry to craft a definition that will fit the context of the phishing practices this bill aims to prohibit.

3.Clarifying language needed for the terms of the bill's private right of action

The language of the bill creates a private right of action for "any person who is either engaged in the business of providing Internet access service to the public or who owns a Web page or trademark and who is adversely affected by a violation of [the Act]. . . ." [Section 22948.3(a) of SB 355 on page 2, lines 38-40.]

The bill also provides that an individual adversely affected by a violation may only sue the direct violator. [Section 22948.3(d) of SB 355 on page 3, lines 17-20.]

Two issues are unclear from this language: (1) whether ISPs must be adversely affected by a violation before bringing suit; and (2) whether any individual who is adversely affected by a violation may sue (as implied in subparagraph (d)), or only those individuals described in subparagraph (a).

The author's staff has clarified that the author intends for an ISP's right of action to attach only when it suffers an adverse effect, and that he intends for all adversely affected individuals to have a private right of action. Committee staff is working with the author's staff to craft language that will make these intentions explicit.

SHOULD THESE PROVISIONS BE CLARIFIED?

4.Should the provision defining "violation" be modified (or deleted)?

The bill provides that multiple violations of the Act will be treated as one violation for purposes of calculating damages when those violations "result[ed] from a single action or conduct." [Section 22948.3(b).] The purpose and scope of this provision is unclear.

One possible interpretation is that the single act of emailing a phishing letter to a list of email addresses is only one violation of the Act, instead of a separate violation for each recipient. This is clearly out of line with the intentions of the Act. Mass emails are frequently used by phishers, since they often must appeal to large numbers of victims in the hope of getting a few responses before taking down their Web site to avoid being caught. There is no reason for mass emails to receive smaller damages than separate emails sent to the same number of victims.

Even assuming the language of this provision may be modified to exclude the circumstance described above, it is not clear how the provision is helpful in assessing

damages under the Act.
SHOULD THIS PROVISION BE DELETED FROM THE BILL? OR SHOULD IT BE MODIFIED TO CLARIFY ITS SCOPE?

5. Should the attorneys' fees provision be limited to prevailing plaintiffs?

The general rule governing attorneys' fees in the United States is that each party must bear the cost of his or her own attorneys' fees, regardless of who prevails in litigation. Fee shifting statutes are enacted only when society considers a statutory or constitutional right important enough to justify fee shifting. And fee statutes may be weighted in favor of "prevailing plaintiffs" when society seeks to encourage vigorous, good faith private enforcement of a right. [See Choate v. County of Orange (2000) 86 Cal. App. 4th 312, 322-23.] This is because making fees available to both parties may allow the party with greater economic resources to use the fees provision as a "hammer" to discourage individual suits.

This bill provides that any prevailing party may seek attorneys' fees and costs. This provision may discourage individuals from enforcing their rights under the Act "because they lack financial resources or because they fear they will have to pay the other side's attorney fees if they lose." [Choate, 86 Cal. App. 4th at 322-23.]

SHOULD THE ATTORNEYS' FEES PROVISION BE AMENDED TO STATE THAT FEES ARE ONLY AVAILABLE TO PREVAILING PLAINTIFFS?

Support: California Alliance for Consumer Protection, Computing Technology Industry Association (CompTIA), Microsoft, Tech Net

Opposition: None Known

HISTORY

Source: Author

Related Pending Legislation: None Known

Prior Legislation: None Known

SB 355 (Murray)
Page 7

****